NSW Health

Privacy Management Plan

Released April 2023

NSW GOVERNMENT

NSW Ministry of Health
1 Reserve Road
St Leonards NSW 2065

Tel. (02) 9391 9000
Fax. (02) 9391 9101
TTY. (02) 9391 9900

www.health.nsw.gov.au

Produced by: NSW Ministry of Health

SHPN (LRS) 220483

ISBN 978-1-76023-239-9

Privacy Management Plan Record of Amendment

No.	Approval date	Reason for amendment

CONTENTS

1. BACKGROUND

NSW Health is responsible for managing and funding health services in a wide range of settings, from multi-purpose health centres in remote communities to large metropolitan teaching hospitals.

There are more than 220 public hospitals and health services in NSW which provide free health care to Australian citizens and permanent residents. Services provided at public hospitals may include emergency care, elective and emergency surgery, medical treatment, maternity services, and rehabilitation programs. These health services are managed through a network of local health districts (Districts), specialty networks, and non-government affiliated health organisations, known collectively as NSW Health.

More detailed information about the structure of NSW Health is available on the NSW Health **website**.

1.1. Privacy management at NSW Health

NSW Health is responsible for the collection, use and management of significant amounts of personal and health information in its operations providing health and medical services to the people of NSW. It is important that both staff and members of the public have access to the necessary information and resources to ensure a consistent and systematic approach to privacy compliance.

The NSW Health Privacy Management Plan is underpinned by the requirements of the *Privacy and Personal Information Protection Act 1998* (PPIP Act) and the *Health Records and Information Privacy Act 2002* (HRIP Act).

NSW Health has developed this Privacy Management Plan (the Plan) in accordance with section 33 of PPIP Act. It sets out NSW Health's commitment to respecting the privacy rights of its staff, patients and other third parties. It also explains NSW Health's policies and procedures in managing personal information under the PPIP Act and health information under the HRIP Act, including how to access and amend personal information, and who to contact in the event of any privacy complaints or concerns.

All NSW Health staff have an obligation to implement the privacy principles established by the PPIP Act and HRIP Act in their work practices, in the course of collecting, managing, using, disclosing, and securing personal and health information.

The ***Privacy Manual for Health Information*** comprehensively sets out how NSW Health manages health information under the HRIP Act.

1.2. NSW Ministry of Health

The NSW Ministry of Health (the Ministry) supports the executive and statutory roles of the Health Cluster and Portfolio Ministers.

The Ministry also has the role of system manager in relation to the NSW public health system, and the operation of public hospitals, community health and other public health services, for the NSW community across the State.

The Ministry coordinates the development of privacy policy for NSW Health and supports a system-wide approach to privacy matters (including complaints, internal reviews, and privacy breaches) to ensure policy consistency across the health system.

1.3. NSW Health organisations

NSW Health comprises:

- A number of state-wide or specialist health services including NSW Ambulance, Health Infrastructure, HealthShare NSW, NSW Health Pathology, eHealth NSW, and Health Protection NSW
- Fifteen local health districts (Districts) providing health services across NSW. There are eight districts covering the Sydney metropolitan region and seven covering rural and regional areas. Districts include hospitals and rural multi-purpose services.
- Two specialty health networks (Justice Health and Forensic Mental Health

Network, and the Sydney Children's Hospitals Network)

- Statutory health corporations (including the Agency for Clinical Innovation, Bureau of Health Information, Clinical Excellence Commission, and Health Education and Training Institute)
- Cancer Institute NSW, established under the *Cancer Institute (NSW) Act 2003,* to lessen the impact of cancer across the State
- Other administrative units of the Health Administration Corporation and all organisations under the control and direction of the Minister for Health or the Secretary, NSW Health.

1.4. Legislative framework

1.4.1. NSW Legislation

Health Records and Information Privacy Act 2002 (NSW) (HRIP Act)

Health Records and Information Privacy Regulation 2022 (NSW)

Health Records and Information Privacy Code of Practice 2005 (NSW)

Independent Commission Against Corruption Act 1988 (NSW)

Privacy and Personal Information Protection Act 1998 (NSW) (PPIP Act)

Privacy and Personal Information Protection Regulation 2019 (NSW)

Government Information (Public Access) Act 2009 (NSW) (GIPA Act)

State Records Act 1998 (NSW)

1.4.2. Commonwealth Legislation

My Health Record Act 2012 (Cth)

Privacy Act 1988 (Cth)

1.5. Key definitions

Collection (of personal information)	How information is acquired by NSW Health. This can include collection of personal information provided verbally, in writing or in a photographic image. Personal information is not ***collected*** if the receipt of the information by the agency is unsolicited.
Collection (Privacy) Notice	A document that informs and notifies a person of what you intend to do with their personal information. The purpose of a collection notice is to provide accessible information to individuals about the use of personal information by the NSW Health organisation and how individuals can access a copy or request amendment of the personal information held by the NSW Health organisation.
Disclosure (of personal information)	To provide personal information to an individual or entity outside of a NSW Health organisation, including sharing (non-health) personal information between NSW Health organisations, with some limited exceptions.
Data breach	Unauthorised access to, and/or the unauthorised use, disclosure or loss of information including personal information, health information or other sensitive or commercial in confidence information.
Information Protection Principles (IPPs) in the PPIP Act and the Health Privacy Principles (HPPs) in the HRIP Act	The IPPs and HPPs regulate the collection, storage, use and disclosure of personal information and health information. The principles also give members of the public a right to request access to their personal or health information or to ask for amendments to that information to ensure it is accurate
Investigative agency	Any of the following: the NSW Ombudsman's office, the Independent Commission Against Corruption (ICAC) or the ICAC inspector, the Law Enforcement Conduct Commission (LECC), the LECC Inspector, Community Services Commission, the Health Care Complaints Commission, the Ageing and Disability Commissioner, the Children's Guardian, the Office of the Legal Services Commissioner, the Inspector of Custodial Services.
Law enforcement agency	The NSW Police Force (or the police force in another State or Territory), the NSW Crime Commission, the Australian Federal Police, the Australian Crime Commission, the NSW Director of Public Prosecutions (DPP) (or DPP of the Commonwealth or another State or Territory), Department of Corrective Services, Department of Juvenile Justice, Office of the Sheriff of NSW.
NSW Health	Refers collectively to NSW Health organisations.
Privacy breach	Refers to any conduct that breaches any of the Information Protection Principles (IPPs) or the Health Privacy Principles (HPPs) (or other relevant privacy legislation) and may also refer to a data breach.
Privacy contact officer	A Privacy Contact Officer (PCO) facilitates compliance with privacy law and NSW Health privacy policy in their organisation.
Privacy obligations	The Information Protection Principles (IPPs), the Health Privacy Principles (HPPs) and any exemptions to those principles that apply to NSW Health.
Staff	Any person working in a casual, temporary, or permanent capacity in NSW Health, including volunteers, students, consultants, contractors, board members and any person performing a public official function whose conduct could be investigated by an investigating authority.

Additional definitions may be found in the ***Privacy Manual for Health Information*** (Part 1).

2. WHAT THIS PLAN COVERS

This Plan addresses the management of both personal information and health information. However, it provides a more detailed discussion of the management of non-health personal information, such as staff information. This is because the management of health information by NSW Health is discussed in detail separately in the ***Privacy Manual for Health Information***.

2.1. Personal information

'Personal information' is defined in section 4 of the *Privacy and Personal Information Protection Act 1998* (PPIP Act).

> *Personal information is information or an opinion (including information, or an opinion forming part of a database, and whether or not recorded in a material form) about an individual whose identity is apparent, or can reasonably be ascertained from the information or opinion.*

Personal information includes a person's name, bank account details, a photograph, or a video. Personal information also includes such things as an individual's fingerprints, retina prints, voice recordings, body samples or genetic characteristics.

Section 4 of the PPIP Act excludes certain types of information from the definition of personal information. The most significant exceptions are:

- Information contained in a publicly available publication
- Information about people who have been dead for more than 30 years
- Information about an individual contained in a public interest disclosure
- Information about an individual's suitability for public sector employment.

Recruitment records and referee reports are not personal information in circumstances where an applicant's information needs to be shared and discussed (with referees and recruitment panels) in relation to their suitability for employment during recruitment. Other recruitment information, for example a referee's personal contact details, will be maintained confidentially and will only be available to relevant staff in the recruitment process.

Section 4A of the PPIPA Act excludes health information from the definition of personal information.

2.2. Health information

Health information is governed by the *Health Records and Information Privacy (HRIP) Act 2002*. It is defined in section 6 of the HRIP Act to mean personal information that is information or an opinion about:

- A person's physical or mental health or disability
- A person's express wishes about the future provision of health services for themselves
- A health service provided, or to be provided, to a person

Any personal information collected for the purposes of the provision of health care will generally be 'health information'.

Health information also includes personal information that is not itself health-related but is collected in connection with providing health services (e.g., contact details and demographic information in a health record).

There are 15 Health Privacy Principles (HPPs) set out in Schedule 1 of the HRIP Act which govern health information in relation to public sector agencies and private sector organisations.

For guidance on the management of health information in NSW Health, refer to the ***Privacy Manual for Health Information***.

3. PERSONAL INFORMATION HELD BY NSW HEALTH

The functions of NSW Health are established primarily under the ***Health Services Act 1997*** and the ***Health Administration Act 1982***. Given the diversity of functions across NSW Health organisations, a wide range of personal and health information is held.

Some of the types of personal information held by NSW Health are discussed below.

3.1. Personal information provided during enquiries

Across NSW Health, staff receive many different types of enquiries from members of the public, private health professionals, staff members and organisations which may be made by phone, email, in writing or in person and include complaints, feedback or human resources matters, fundraising, coordinating volunteers or other management related enquiries, for example.

When making these enquiries, people may provide NSW Health staff with personal and health information. This could include names, contact details, opinions about other persons, health conditions and illnesses, family relationships, housing or tenancy information, work history, education, and criminal history.

NSW Health collects personal information that is reasonably necessary for the purpose of the collection (relevant, and not excessive) and this may vary on a case-by-case basis and be dependent on the nature of the individual enquiry. Sufficient information will be collected to accurately record the management of the matter. NSW Health will use and disclose such personal information for the purpose it was provided or where lawfully required or authorised.

In most cases where the enquiry relates to patient care, the information collected will be health information, which is governed by the HRIP Act and the ***Privacy Manual for Health Information***.

3.2. Staff records

3.2.1. What information is collected?

Personal and health information of staff is collected, stored, used, and disclosed in accordance with the PPIP Act and the HRIP Act. Staff records include:

- personal contact details and emergency contacts
- payroll, attendance and leave records
- records of gender, ethnicity and disability
- medical conditions
- workers compensation records
- workplace health and safety records
- bank account, superannuation fund and tax file numbers
- performance and development records
- training records
- secondary employment
- conflicts of interest

3.2.2. Use of staff information

NSW Health uses staff records for managing processes associated with the employment relationship with NSW Health and general human resources management and planning functions, including:

- Recruitment, staff development and training
- Payroll, rostering, deployment, and associated processes
- Risk analysis and management, benchmarking, reporting, research, evaluation and analysis, auditing and quality assurance activities directly related to the NSW Health workforce or employment in NSW Health
- Workforce strategic planning, skills analysis and the monitoring and analysis of secondary employment of NSW Health staff to inform resource planning and redeployment options
- Data analysis to develop and improve human capital services
- Sharing relevant organisational and employment data with other NSW Health systems used in human resource management and planning
- Managing performance and development

- Managing staff conduct, complaints and workplace investigations
- Informing staff about benefits and opportunities, for example, employment and career opportunities, learning and development, diversity and inclusion programs, and other opportunities available to employees, including dissemination of news and information directly related to employment.

3.2.3. Disclosure of staff information to service providers and for other purposes

Staff personal information may be disclosed to service providers and contractors where necessary to support the uses outlined above for purposes directly related to the management and planning of the NSW Health workforce.

NSW Health may also disclose staff personal information where authorised or required to do so by law, including:

- in response to a subpoena, summons, search warrant, or court orders
- to a law enforcement agency if there are reasonable grounds to believe that an offence has or may have been committed
- for purposes required by child protection, taxation, employment, other investigative agencies or work health and safety legislation or investigative agencies
- for purposes related to staff complaints, conduct or workplace investigation matters
- where the disclosure is necessary to prevent or lessen a serious and imminent threat to the life or health of staff or another person
- in relation to matters that have been referred to the Industrial Relations Commission of NSW.

Staff may contact **EHNSW-HCMInfo@health.nsw.gov.au**, if they have any queries about their employment records.

3.2.4. Disclosure of staff information to members of the public

The names of staff included in a health record or other work-related files are routinely provided to members of the public who request access to information held about them by NSW Health.

Similarly, disclosure of an email address containing a staff member's name for work related purposes is a necessary part of routine business.

However, there may be exceptional circumstances where staff details are not disclosed to members of the public. NSW Health can withhold staff details if there are grounds to do so under the Government Information (Public Access) Act (GIPA Act). For example, staff names are not disclosed if to do so could reasonably be expected to expose a staff member to a risk of harm. For more information, see the ***Privacy Manual for Health Information***.

3.3. Business records

NSW Health maintains business records which contain personal information including contact details for public officials in other government entities, as well as contracted service providers, vendors, suppliers, and other third-party organisations.

3.4. CCTV and surveillance

NSW Health installs and maintains closed circuit television (CCTV) cameras on premises for a number of purposes, including:

- to ensure the safety and security of staff, patients, and visitors whilst on NSW Health premises
- to protect assets and property of NSW Health and others
- to assist in crime prevention and aid in the investigation of criminal activity or other misconduct
- to assist NSW Health to manage its facilities, such as its car parks, waiting areas and hospitals, for example.

Prominent signage notifies all staff, patients, and members of the public of the use of CCTV and that they may be under camera surveillance.

Access to the CCTV images is controlled and secure to ensure that only authorised staff have access to any images.

For more detail see Chapter 13 of the NSW Health ***Protecting People and Property Manual***.

4. HOW THE INFORMATION PROTECTION PRINCIPLES APPLY

The PPIP Act sets out 12 Information Protection Principles (IPPs), summarised in 5.1-5.5 below. NSW Health must follow these principles in relation to collecting, storing, using, and disclosing personal information.

Specific applications of these principles have been incorporated into NSW Health policies and procedures relating to collection, storage, use or disclosure of personal information.

NSW Health organisations use a variety of paper-based and electronic systems for managing information. NSW Health organisations follow strict rules in storing and securing personal information in all its formats to protect it from unauthorised access, disclosure, loss, or other misuse.

This includes ensuring records are appropriately secured, and where appropriate, access to records is auditable in the event of a privacy breach.

Further information is available from:

NSW Health Policy Directive *Communications - Use & Management of Misuse of NSW Health Communications Systems* (**PD2009_076**).

NSW Health Policy Directive *Electronic Information Security* (**PD2020_046**).

Information in relation to the Health Privacy Principles (HPPs) can be found in the ***Privacy Manual for Health Information***.

4.1. Collection

Lawful

NSW Health organisations will only collect personal information for a lawful purpose, which is directly related to our functions or activities and necessary for that purpose.

Direct

NSW Health organisations will only collect personal information directly from the person concerned unless they have authorised collection from someone else or the person is under the age of 16 and the information has been provided by a parent or guardian.

Open

NSW Health organisations inform people why their personal information is being collected, what it will be used for, and to whom it will be disclosed. We tell people how they can access and amend their personal information and the consequences if they decide not to give their personal information to us.

Relevant

NSW Health organisations ensure that personal information is relevant, accurate, is not excessive and does not unreasonably intrude into the personal affairs of people.

4.2. Storage

Secure

NSW Health organisations store personal information securely, keep it no longer than necessary and destroy it appropriately. We protect personal information by taking such security safeguards as are reasonable in the circumstances, against loss, unauthorised access, use, modification, or disclosure.

4.3. Access and Accuracy

Transparent

NSW Health organisations are transparent about the personal information we store about people, why we use the information and about the right to access and amend it.

Accessible

NSW Health organisations allow people to access their own personal information without unreasonable delay or expense.

Correct

NSW Health organisations allow people to update, correct or amend their personal information where necessary.

4.4. Use

Accurate

NSW Health organisations will take such steps that are reasonable in the circumstances to ensure that personal information is relevant, accurate and up to date before using it.

Limited (Use)

NSW Health organisations can only use personal information for the purpose it was collected unless they can rely on one of the following statutory exceptions:

- the person consents to the use for that other purpose
- the other purpose is directly related to the purpose for which the information was collected
- disclosure is necessary to prevent a serious and imminent threat to the health and safety of the individual or any person
- where otherwise required or authorised to use the information.

4.5. Disclosure

Restricted (Disclosure)

NSW Health organisations can disclose personal information with a person's consent.

NSW Health organisations can also disclose personal information if one of the following statutory exceptions applies:

- if disclosure is directly related to the purpose for which the information was collected and there is no reason to believe the person would object
- the person has been made aware that information of that kind is usually disclosed
- if disclosure is necessary to prevent a serious and imminent threat to the health and safety of the individual or any person
- where otherwise required or authorised to disclose the information.

Special safeguards for sensitive personal information

NSW Health organisations will take particular care not to disclose sensitive personal information without a person's express consent. For example, this includes information about ethnic or racial origin, political opinions, religious or philosophical beliefs, sexual activities, or trade union membership. We will only disclose sensitive information to deal with a serious or imminent threat to the health and safety of the individual or another person or if another exemption applies (see Section 9, below).

5. HOW TO ACCESS AND AMEND INFORMATION ABOUT YOU

Members of the public, staff and other third parties have rights to access personal and health information about them held by NSW Health and to request amendments to their personal and health information. These rights can be exercised by informal or formal processes.

5.1. Informal request

A person seeking to access or amend their own personal or health information can make an informal request to the staff member or team managing their information. This request does not need to be made in writing. If a person is unhappy with the outcome of their informal request, they can make a formal application.

5.2. Formal applications

A person can make a formal application to the manager of the business unit holding the information. More complex requests may be made directly to the **Privacy Contact Officer** for the relevant NSW Health organisation by email, fax, or post.

The application should:

- Include the person's name and contact details
- State whether the person is making the application under the PPIP Act or the HRIP Act
- Explain what personal or health information the person wants to access or amend
- Explain how the person wants to access or amend it.

The person managing the request will aim to respond to the formal application within 20 working days. They will contact the applicant to advise how long the request is likely to take, particularly if it may take longer than expected.

If the applicant thinks the NSW Health organisation is taking too long to deal with the request, the applicant may contact the relevant Privacy Contact Officer, request an update, and time frame for the matter to be dealt with. If the applicant remains unsatisfied, they have the right to seek an internal review under the PPIP Act or HRIP Act, or make a complaint directly to the Privacy Commissioner.

5.3. Fees

NSW Health organisations cannot charge people to lodge their request for access to their personal information, but reasonable fees may be charged for copying or inspection of records, if the fees are notified and explained to applicants.

It should be noted that there is a charging policy with respect to health records (see: *Health Records and Medical/Clinical Reports - Charging Policy* (**PD2006_050**) and *Health Records and Medical/Clinical Reports - Rates* (**IB2019_036**)).

A NSW Health organisation has discretion to discount or waive fees in certain circumstances, e.g., financial hardship.

5.4. Limits on rights to access information

If there is personal information about other individuals or confidential information about third parties in any records identified by searches, then the request will be more complex to manage. It may be necessary to redact third party information and limit access to information that may cause harm. Requests of this nature ought to be referred to the Privacy Contact Officer to ensure that the privacy and confidentiality of third parties can be properly considered.

Further guidance on access to, and amendment of health information is provided in Section 12 of the ***Privacy Manual for Health Information***. While a person is presumed to have the right to access information about them (or the person they represent), the GIPA Act provides a legislative basis to refuse access to certain information where there are public interest considerations around the disclosure of the information that might be personal, sensitive, or commercial in confidence.

6. COMPLAINTS, INTERNAL REVIEWS AND REMEDIES

6.1. Privacy Complaints and Internal Review

An individual who is aggrieved by the handling of their personal or health information may make a complaint to the NSW Health organisation. A complainant may also make a complaint directly to the NSW Privacy Commissioner.

A NSW Health organisation that receives such a complaint is required to consider whether to undertake a privacy internal review.

Some complaints may be dealt with informally or under the procedures of the NSW Health Policy Directive *Complaints Management Policy* (**PD2020_013**), instead of through a privacy internal review, in appropriate circumstances or at the request of the complainant.

A request for a privacy internal review can be made where an individual believes that a NSW Health organisation has:

- breached any of the HPPs
- breached any of the IPPs
- breached any code of practice or public interest direction made under either of the Acts applying to NSW Health, or
- disclosed information on a public register, except in accordance with section 57 (PPIP Act only).

An individual may also complain on behalf of someone else if they are authorised to act on their behalf (for example, with the applicant's consent or if they are a parent, guardian, or executor).

In addition, an individual may be aggrieved by the handling of someone else's personal or health information and such a complaint may also require a privacy internal review.

Sometimes a third party can also be affected by a disclosure. However, careful consideration would then need to be given to what extent, if any, it would be appropriate to provide information relevant to the complaint to a third party given that to do so might cause additional privacy breaches.

Under s53(3) of the PPIP Act, an application for an internal review must:

- Be addressed to the appropriate NSW Health organisation
- Be in writing
- Specify an address within Australia to which a notice can be sent
- Be lodged within 6 months from when the applicant became aware of the conduct the subject of the application (however, in some circumstances NSW Health may consider a late application for internal review).

6.2. Privacy internal review process

An application for an internal review will be dealt with in accordance with the *NSW Health Privacy Internal Review Guidelines* (**GL2019_015**). A privacy internal review application form is provided at Appendix 4 of the Guidelines.

The review will be managed by the **Privacy Contact Officer** for the NSW Health organisation, or another suitably qualified officer of that organisation.

The review will be completed as soon as is reasonably practical, and within 60 days from the date the application is received.

NSW Health organisations may seek advice from the Ministry of Health before finalising any privacy internal review, to ensure any significant legal, policy, industrial or safety issues, for example, have not been overlooked.

When the internal review is completed, the Privacy Contact Officer will notify the applicant in writing (within 14 days) of:

- The findings of the review
- The reasons for the finding, described in terms of the Information Protection and/or Health Privacy Principles
- Any action the NSW Health organisation proposes to take
- The reasons for the proposed action (or no action), and
- The applicant's entitlement to have the findings and the reasons externally reviewed by the NSW Civil and Administrative Tribunal (NCAT).

The NSW Health organisation will also send a copy of the finalised internal review report to the NSW Privacy Commissioner.

Statistical information about the number of privacy internal reviews conducted by each NSW Health organisation is maintained for the organisation's Annual Privacy Report.

Further guidance for members of the public on the internal review process can be found on the Information and Privacy Commission NSW's **website**.

6.3. Remedies

The outcomes of an internal review where a breach of privacy has occurred may include:

- Provision of an apology
- Provision of undertakings that the conduct will not occur again
- Changes to procedures to prevent similar breaches occurring again
- Agreement to conduct training and education of staff
- Compensation, in limited circumstances, if supported by evidence of loss or damage.

If the applicant is dissatisfied with the findings of the review and the health service's response, including any offer of compensation, the PPIP Act provides a right to lodge an appeal to the NSW Civil and Administrative Tribunal within 28 calendar days from receipt of the internal review report. There are maximum financial limits for compensation claims.

For more information, please refer to the Information and Privacy Commission NSW **website**.

6.4. Internal reviews and the role of the Privacy Commissioner

As the provisions of Part 5 of the PIPP Act include the oversight functions of the Privacy Commissioner, NSW Health has certain obligations during the conduct of internal reviews.

Under section 54(1)(a) agencies must notify the Privacy Commissioner as soon as practicable after they receive the application.

Under section 54(1)(b) agencies must *"keep the Privacy Commissioner informed of the progress of the internal review."*

Section 54(1)(c) states that agencies must *"inform the Privacy Commissioner of the findings of the review and of the action proposed to be taken by the agency in relation to the subject matter of the application."*

The Privacy Commissioner does not take sides in internal reviews of complaints and is not a party in proceedings in the Tribunal.

The oversight function aims at encouraging investigations to produce quality outcomes, adequately deal with privacy issues and lead to better compliance with the legislation.

For more information on the role of the Privacy Commissioner, please refer to the Information and Privacy Commission NSW **website**.

6.5. External Review by the NSW Civil and Administrative Tribunal (NCAT)

A person must seek an internal review before they have the right to seek an external review from the NSW Civil and Administrative Tribunal (**NCAT**). An applicant can apply to the Tribunal for an external review of the conduct which was the subject of the internal review. A person has 28 days from completion of the internal review to seek an external review.

The Tribunal has the power to make binding decisions on an external review. More information on how to request an external review is available from the NCAT Registry. The Tribunal does not provide legal advice; however, their website has general information about the process of seeking an external review.

For more information, please refer to the NSW Civil and Administrative Tribunal **website**

.

7. MANAGEMENT OF DATA BREACHES

7.1. Data breach notification requirements

Anyone who has concerns about a privacy breach or inappropriate access to their personal information should contact the privacy contact officer at the relevant NSW Health organisation.

Serious data breaches will be notified by the NSW Health organisation to the Ministry of Health.

NSW Health organisations apply the Voluntary Data Breach Notification scheme of the NSW Information and Privacy Commission. A risk analysis is conducted by the NSW Health organisation to determine whether the breach is to be notified to:

(a) persons affected by the data breach; and

(b) the NSW Privacy Commissioner.

In assessing seriousness of the breach, the following will be considered:

- The type of data that has been breached. Does it include financial or other sensitive categories of data? Are there other characteristics of the data that could pose a high risk?
- The data context. Does the breach affect data that would normally be publicly available, or is the data known to be very poor quality that if used could create risk to individuals?
- How easy it would be for individuals to be identified from this data
- Whether the data breach complicated by the involvement of other government agencies, contractors, or organisations.
- The circumstances of the breach. For example, a single incident (such as the loss of a device, or unintended error), a malicious attack that poses an ongoing risk, or data that was altered in a way that may pose a risk to the individuals to whom the data relates.

7.2. Commonwealth mandatory notification requirements

The Commonwealth *Privacy Act 1988* (the Privacy Act) imposes mandatory requirements to report serious breaches of privacy to the Office of the Australian Information Commissioner (OAIC) and affected parties.

This does ***not*** apply to most information under the control of NSW Health as NSW Health organisations are largely exempt from the requirements of the Privacy Act, but NSW Health organisations ***are*** subject to mandatory data breach notification requirements for breaches relating to Tax File Numbers (TFNs) and the My Health Record system.

NSW Health organisations may seek guidance on whether a privacy breach reaches the reporting threshold, from the Ministry of Health, before any notifications are made to the Office of the Australian Information Commissioner or the Australian Digital Health Agency.

Tax file numbers (TFNs)

Serious data breaches involving Tax File Numbers must be notified to the Office of the Australian Information Commissioner. The Privacy (Tax File Number) Rule 2015 requires that Tax File Number recipients (like NSW Health) must take reasonable steps to ensure that:

(a) all staff are aware of the need to protect individuals' privacy when handling Tax File Number information, and

(b) all staff who collect or access Tax File Number information are aware of:

(i) the circumstances where Tax File Number information may be collected

(ii) the prohibitions on the use and disclosure of Tax File Number information

(iii) the need to protect individuals' privacy when handling Tax File Number information, including under the TFN Rule and under the Privacy Act

(iv) the penalties or other sanctions that apply for breaching the TFN Rule or applicable laws relating to the handling of Tax File Numbers.

My Health Record

Under section 75 of the *My Health Records Act 2012* (Cth), health services are required to notify the Australian Digital Health Agency of data breaches involving My Health Record. The Australian Digital Health Agency, rather than NSW Health organisation, is required to notify any patients affected by a confirmed data breach involving My Health Record.

A data breach occurs if there is unauthorised collection, use or disclosure of information included in a My Health Record. Unauthorised uses may include improperly accessing, viewing, modifying or deleting information included in a person's My Health Record.

Viewing a person's My Health Record for purposes unrelated to provision of healthcare is a notifiable data breach.

8. PRIVACY EXEMPTIONS AND SPECIAL PROVISIONS

Some of the exemptions to the Information Protection Principles (IPPs) are discussed below. Different exemptions may apply for an IPP and its equivalent HPP.

When considering whether an exemption applies, it is therefore important to determine if the information is only personal information or if it also includes health information. If the information is health information, it is necessary to refer to the ***Privacy Manual for Health Information*** for further guidance.

When considering whether an exemption may apply to a situation, the wording of the exemptions contained within the PPIP Act should be carefully considered, and guidance sought from the **Privacy Contact Officer**. Sections 22 to 28 of the PPIP Act detail specific exemptions to the IPPs. Common exemptions include unsolicited personal information and personal information used for law enforcement or investigative purposes.

8.1. Lawfully authorised or with consent

NSW Health organisations may not be required to comply with the IPPs if the conduct in question, such as a use or disclosure of personal information, is authorised or required by law, or if the person has expressly consented.

8.2. Emergency provisions

Under s27D of the PPIP Act, exemptions apply to handling of personal information in a stage of emergency (including natural disasters such as bushfires, for example) as defined by the *State Emergency and Rescue Management Act 1989*. However, under this exemption, if a NSW Health organisation collects, uses or discloses personal information relying on the emergency exemption, it must not hold the information for longer than 18 months, unless extenuating circumstances apply, or consent has been obtained.

8.3. Legal matters, complaints, investigations, law enforcement requirements

Exemptions may also apply in the following circumstances:

Collection:

- When collecting information in connection with legal proceedings (whether or not actually commenced) before any court or tribunal
- When collecting information during investigation or management of a complaint or a matter that could be made or referred to an investigative agency, or which has been referred to the NSW Health organisation by an investigative agency
- When compliance with the IPPs in relation to collection would prejudice the interests of the individual to whom the information relates.

Use:

- When the use of the information is for a purpose (other than the purpose for which it was collected) that is reasonably necessary for law enforcement purposes
- When the use of the information is reasonably necessary to enable investigation or management of a complaint which could be made or referred to an investigative agency, or which has been referred to the health organisation by an investigative agency. This could include conduct related to employment matters, healthcare, or allegations of corrupt conduct, for example.

Disclosure:

- When the disclosure is made in connection with proceedings for an offence, or for law enforcement purposes
- When the disclosure is made to a law enforcement agency for the purposes of ascertaining the whereabouts of a person who has been reported missing
- Where sensitive information is required to be disclosed for law enforcement purposes where there are reasonable grounds to believe an offence may have been, or may be committed
- When the disclosure is to an investigative agency.

- When the information is disclosed by a NSW Health organisation to another NSW Health organisation under the administration of the Minister for Health, if the disclosure is for the purposes of informing that Minister about any matter within that administration
- When the information is disclosed by the NSW Health organisation to any public sector agency under the administration of the Premier, if the disclosure is for the purposes of informing the Premier about any matter
- Information can be collected, used or disclosed where reasonably necessary to enable inquiries to be referred between the public sector agencies. Under the PPIP Act, this could include an exchange of information between the Ministry of Health and Local Health Districts in relation to a complaint or enquiry, for example.

8.4. Public Registers

The PPIP Act governs how NSW Health organisations manage personal and health information in public registers (see Part 6 of the PPIP Act – Public Registers).

Under the legislation, an agency responsible for keeping a public register must not disclose any personal information kept in the register unless satisfied that it is to be used for a purpose relating to the purpose of the register, or the Act under which the register is kept. A person applying to inspect information in the public register may be required to provide a statutory declaration as to the intended use of any information obtained.

A person whose information is contained in a public register may request the agency responsible for the register to have their information removed from public availability on the register and not disclosed to the public.

In most cases, personal and health information held by a NSW Health organisation is not publicly available. However, there are some circumstances where personal information may be held on registers by a NSW Health organisation which are available to the public. For example, NSW Health's Tobacco Retailer Notification Scheme requires tobacco retailers to provide information including their trading name and business address and the name and address of the owners and directors of the business.

A person who wishes to access or request the suppression of personal or health information contained in a public register managed by a NSW Health organisation should contact the relevant business unit responsible for the register to discuss their request.

8.5. Public Interest Directions

Under section 41 of the PPIP Act, the Privacy Commissioner can issue Public Interest Directions to waive or modify the requirement for a public sector agency to comply with an IPP. Details about current Public Interest Directions can be found on the Information and Privacy Commission NSW **website**.

The general intent is that Public Interest Directions are to apply temporarily. If a longer-term waiver or change in the application of an IPP is required, then a Code of Practice may be more appropriate.

An example is the Public Interest Directions relating to the Human Services Dataset that have been issued under the PPIP and HRIP Acts. This Direction has been prepared to facilitate information sharing and funding across government that is focused on interventions to improve the long-term outcomes for vulnerable children and their families. These directions were made on 9 July 2021 and the Project will use Human Services data across government to design and deliver better government services for vulnerable children and young persons and their families.

NSW Health was consulted on this Public Interest Direction as it relates to the management of health information.

8.6. Privacy Codes of Practice

A Privacy Code of Practice is a legal instrument which allows a public sector agency or organisation to make changes to an IPP or provisions that deal with public registers.

Codes of Practice can be made to assist in the implementation of different government programs, that may require privacy exemptions to recruit participants, exchange information between agencies or to provide access to certain information that might be in the public interest, for example.

Privacy Codes of Practice cannot be stricter than the principles and do not provide blanket exemptions to the principles. Agencies (including NSW Health) must consult the Privacy

Commissioner when preparing Privacy Codes of Practice to modify the application of one or more Information Protection Principles (IPPs) or the public register provisions of the PPIP Act or specify how they are to be applied to particular activities or classes of information.

It is recommended that the Privacy Commissioner is provided with a business case setting out the need for a Code and any supporting material before any draft Codes are prepared for approval.

Codes of Practice that modify Health Privacy Principles (HPPs) are referred to as Health Privacy Codes of Practice. Privacy Codes of Practice and Health Privacy Codes of Practice are listed on the Information and Privacy Commission NSW **website**.

9. SUPPORT TO IMPLEMENTATION

9.1. Staff training and education

NSW Health provides regular training and education seminars to staff to inform them of their responsibilities under the Privacy Acts.

New staff members in NSW Health organisations receive **mandatory privacy training** as part of their induction and orientation process.

Privacy news and updates are communicated to all staff on a regular basis. Other strategies adopted by NSW Health organisations to promote general privacy awareness and education within NSW Health organisations may include:

- Staff are provided with access to this Plan and relevant resources to assist with education on privacy obligations, including the ***Privacy Leaflet for Staff***.
- A de-identified summary of privacy internal review matters is reported annually on NSW health organisation websites.
- Privacy issues are identified and addressed during development and implementation of any new systems
- Privacy notices are prepared as a standard inclusion in all projects where personal information will be collected
- Provision of regular privacy training and highlighting of privacy obligations (for example during Privacy Awareness Week)
- Dedicated Privacy Officers across NSW Health provide tailored advice to staff to support them in understanding and meeting their privacy obligations. For example, the Privacy Officer can provide advice about:
    - Whether personal or health information is being collected, used, or disclosed for a lawful purpose
    - Whether or not the collection of that personal information is reasonably necessary for the specified purpose,
    - Whether any exemptions apply,
    - How to manage complaints, breaches, and requests for internal review
    - The preparation of collection notices and privacy undertakings
- Liaising with the NSW Ministry of Health with issues or queries that arise and cannot be resolved locally.
- Conducting or commissioning Privacy Impact Assessments, to help staff to identify and minimise privacy risks when starting a new project or making changes to existing initiatives.

9.2. Public awareness

NSW Health promotes public awareness of privacy obligations by:

- publishing the NSW Health Privacy Management Plan publicly on the NSW Health website
- publishing all policies, collection notices and privacy information sheets on NSW Health organisation websites and referring to the Plan in privacy notices
- maintaining a dedicated privacy page for all privacy resources and privacy contacts across NSW Health organisations
- Providing privacy contact officers across NSW Health organisations to manage privacy related issues / complaints / investigations
- Making patients, staff members and members of the public aware of the privacy obligations when completing forms that collect personal and health information.
- Telling people about the Plan when answering queries about personal information
- Referring enquiries to the Privacy Contact Officer for the NSW Health organisation where appropriate.

An Information Sheet explaining how personal information is handled by NSW Health is available at Appendix 1 (section 13.1).

The ***NSW Health Privacy Leaflet for Patients*** is available from the NSW Health website and explains how health information is handled by NSW Health (the Leaflet can also be ordered from the State print vendor if hardcopies are required).

Where the public has additional questions, they are encouraged to contact the NSW Ministry of Health Privacy Contact Officer via email **MOH-privacy@health.nsw.gov.au**

or the Privacy Commissioner via:

Office
Level 15, McKell Building
2-24 Rawson Place,
Haymarket NSW 2000

Postal Address
GPO Box 7011
Sydney NSW 2001

Email: **ipcinfo@ipc.nsw.gov.au**

Phone: 1800 472 679

10. NSW HEALTH POLICIES AND RESOURCES

Privacy Internal Review Guidelines

The *NSW Health Privacy Internal Review Guidelines* (**GL2019_015**) provide guidance and information about the internal review process for NSW Health organisations.

Privacy Manual for Health Information

The ***Privacy Manual for Health Information*** governs the management of health information (as opposed to general personal information), as required by the HRIP Act. The Privacy Manual for Health Information is the primary privacy policy source for NSW Health, given that the core business of NSW Health involves managing a large volume of health information.

Subpoenas

The NSW Health Policy Directive *Subpoenas* (**PD2019_001**), outlines legislative provisions and procedures to be followed when the Ministry of Health and public health organisations are required to produce documents and information in response to a subpoena or court order.

NSW Health Code of Conduct

NSW Health Code of Conduct (**PD2015_049**) defines standards of ethical and professional conduct that are required of everyone working in NSW Health in any capacity, the outcomes we are committed to, and the behaviours which are unacceptable and will not be tolerated. The intent of the Code is to provide a framework to promote ethical day-to-day conduct and decision-making, including obligations to maintain the security of confidential information. Section 4.5 of the Code of Conduct includes requirements for observing the privacy, confidentiality and security of information obtained during employment within NSW Health.

Electronic Information Security Policy

The NSW Health Policy Directive *Electronic Information Security* (**PD2020_046**) requires all users of NSW Health electronic information systems and assets to uphold confidentiality and protect information entrusted to them. Information security measures and controls must be developed and implemented to ensure privacy of personal information is preserved, confidentiality of information is protected, security and integrity of information is maintained, and availability of information is assured.

NSW Cyber Security Policy

The **NSW Cyber Security Policy** outlines the mandatory requirements to which all NSW government departments and Public Service Agencies must adhere, to ensure that cyber security risks to their information and systems are appropriately managed. Agencies must establish effective cyber security policies and procedures and embed cyber security into risk management practices and assurance processes.

NSW Health Data Governance Framework

The NSW Health Guideline *NSW Health Data Governance Framework* (**GL2019_002**) outlines the roles and responsibilities involved in data governance and the structures to be put in place to ensure effective and consistent management of the data assets of NSW Health.

Incident Management

NSW Health is committed to learning from incidents. The NSW Health Policy Directive *Incident Management* (**PD2020_047**) provides direction for consistency in managing and effectively responding to clinical and corporate incidents and acting on lessons learned and is in compliance with the requirements of the *Health Administration Act 1982* (NSW).

Managing Misconduct

The NSW Health Policy Directive *Managing Misconduct* (**PD2018_031**) sets out the requirements for managing potential and/or substantiated misconduct by staff of the NSW Health Service and by visiting practitioners.

Communications – Use & Management of Misuse of NSW Health Communications Systems

The NSW Health Policy Directive *Communications - Use & Management of Misuse of NSW Health Communications Systems* (**PD2009_076**) provides guidance and direction about the mechanisms required to minimise inappropriate use and the controls required to monitor the use of NSW Health communications systems and devices.

Corrupt Conduct – Reporting to the Independent Commission Against Corruption (ICAC)

The NSW Health Policy Directive *Corrupt Conduct - Reporting to the Independent Commission Against Corruption (ICAC)* (**PD2016_029**) articulates the requirements for NSW Health Principal Officers to report suspected corrupt conduct to the ICAC.

Significant Legal Matters and Management of Legal Services

The NSW Health Policy Directive *Significant Legal Matters and Management of Legal Services* (**PD2017_003**) will ensure that NSW Health entities notify the General Counsel of the NSW Ministry of Health of Significant Legal matters and adhere to relevant NSW Health and NSW Government policies when involved in legal matters and proceedings. Adherence is necessary to ensure that the State and its agencies are appropriately and effectively represented, and Government advised of matters involving substantial costs or state-wide precedents.

Protecting People and Property Manual

The ***Protecting People and Property Manual*.** outlines NSW Health policy on key aspects of personal and property security that assist NSW Health organisations to maintain an effective security program that is based on a structured, ongoing risk management process, consultation, appropriate documentation, and record keeping and regular monitoring and evaluation.

10.1. NSW Health privacy links

NSW Health Patient privacy webpage
https://www.health.nsw.gov.au/patients/privacy/Pages/default.aspx

NSW Health Privacy Leaflet for Patients
https://www.health.nsw.gov.au/patients/privacy/Pages/privacy-leaflet-for-patients.aspx

NSW Health Privacy Leaflet for Staff
https://www.health.nsw.gov.au/patients/privacy/Pages/privacy-information-for-nsw-health-staff.aspx

11. APPENDICES

11.1. Privacy information sheet for personal information

NSW Health

Privacy and Personal Information

Information Sheet

NSW Health is committed to treating your personal information in accordance with privacy law. This leaflet explains how and why we collect personal information about you, how you can access your information, and how your information may be used within the NSW public health service or disclosed to other parties.

The Privacy and Personal Information Protection Act 1998

The *Privacy and Personal Information Protection Act* (PPIP Act) explains how NSW government agencies, including NSW Health, must manage personal information. The PPIP Act offers the people of NSW enforceable privacy rights. It gives you the opportunity to make a complaint about a public sector agency if you are concerned that it has misused your personal information.

What do 'Privacy' and 'Personal Information' mean?

There is no simple definition of privacy. It can mean the right to a sense of personal freedom, the right to have information about oneself used fairly and appropriately, and a 'right to be left alone.' Many people confuse privacy with secrecy or confidentiality, but privacy is broader than both.

The fair use of 'personal information' is just one aspect of this broader concept of 'privacy.' Personal information is any information or opinion about an identifiable person. This includes records containing your name, address, gender, or physical information like fingerprints, body samples or your DNA.

The 12 Rules of Personal Information Protection

All NSW Health organisations must comply with the Information Protection Principles (IPPs) unless they have a lawful exemption. They are summarised here:

Collection

Lawful (IPP 1)

When NSW Health collects your personal information, the information must be collected for a lawful purpose. It must also be directly related to the organisation's activities and necessary for that purpose.

Direct (IPP 2)

Your information must be collected directly from you unless you have given your consent otherwise.

Open (IPP 3)

You must be informed that the information is being collected, why it is being collected and who will be storing and using it. We should also tell you how you can see and correct this information.

Relevant (IPP 4)

NSW Health must ensure that the information is relevant, accurate, up-to-date, and not excessive. The collection should not unreasonably intrude into your personal affairs.

Storage

Secure (IPP 5)

Your information must be stored securely, not kept any longer than necessary, and disposed of appropriately. It should be protected from unauthorised access, use or disclosure.

Access

Transparent (IPP 6)

The organisation must provide you with enough details about what personal information they are storing, why they are storing it and what rights you have to access it.

Accessible (IPP 7)

The organisation must allow you to access your personal information without unreasonable delay and expense.

Correct (IPP 8)

The organisation must allow you to update, correct or amend your personal information where necessary.

Use

Accurate (IPP 9)

NSW Health must make sure that your information is accurate before using it.

Limited (IPP 10)

NSW Health can only use your information for the purpose for which it was collected, for a directly related purpose, or for a purpose to which you have given your consent. It can also be used to deal with a serious and imminent threat to any person's health or safety.

Disclosure

Restricted (IPP 11)

NSW Health can only disclose your information with your consent or if you were told at the time, we collected it from you that we would do so, or if it is for a purpose that is directly related to the purpose for which the information was collected, and we do not think that you would object. Your information can also be used without your consent to deal with a serious and imminent threat to any person's health or safety, or for other lawfully authorised purposes.

Safeguarded (IPP 12)

NSW Health can only disclose your sensitive personal information without your consent to deal with a serious and imminent threat to any person's health or safety. Sensitive information may be about your ethnic or racial origin, political opinions, religious or philosophical beliefs, health or sexual activities or trade union membership.

What to do if you think your privacy has been breached

If your complaint is about your personal information held by a NSW Health organisation and you are aggrieved by the conduct, you may seek an Internal Review. An Internal Review is an internal investigation that NSW Health is required to conduct when you make a privacy complaint, in the form of a valid application.

An internal review application form is available in the NSW Health Privacy Internal Review Guidelines at Appendix 4.

Sometimes an internal review is not appropriate, but this can be managed according to the circumstances of the complaint.

Contact us

If you have questions or a complaint about the privacy of your personal information, please contact the **Privacy Contact Officer** for the relevant NSW Health organisation.

This information sheet focuses on personal information, such as information collected from members of the public and staff records.

For details on how we manage the health information of patients, please see the *NSW Health Privacy Leaflet for Patients*, available from **www.health.nsw.gov.au/patients/privacy/Pages/privacy-leaflet-for-patients.aspx**

For questions about this publication, please contact:

NSW Ministry of Health
1 Reserve Road
St Leonards NSW 2065

Tel. (02) 9391 9000
Fax. (02) 9391 9101
TTY. (02) 9391 9900

MOH-Privacy@health.nsw.gov.au